Bonhomme, Penny

From: Susan Israel [redacted]
Sent: Tuesday, March 20, 2012 3:42 PM
To: PHC Testimony
Subject: Additional Testimony for SB 368

To the Committee on Public Health March 19, 2012

Additional Testimony in support of S.B. 368

Submitted by Susan Israel, MD

Re: HITE-CT Consumer Authorization and Consent Policy and its proposed Privacy and Security Audit Policy, and CT laws HB 6652, PA 11-61; HB 6678, PA 09-232; PA 10-117

This was written prior to 368, but hopefully gives background for its passage. The PH Committee office has supportive information and copies of the legislation and DPH policies quoted which may be scanned and put online.

HITE-CT, the Health Information Technology Exchange of Connecticut, is being formed under the Department of Public Health for the exchange of patient electronic medical records. The plan is for physicians, other providers and hospitals to join the exchange to make their patient records available to all providers and the Public Health Dept. for treatment, payment and operations. With their current Opt-out policy, patients cannot control who can access their records, nor even keep their records out of the exchange completely. Ideally, patients should control, not only which providers can access their records, but also which *businesses* and public agencies (except in an emergency) can see their records. As per Dr. Deborah Peel of Patient Privacy Rights (*Wall Street Journal*, 1/23/12), there *are* existing technologies to allow patients to set default rules electronically for how their data will be exchanged, to whom, and whether "Sensitive" information will be removed. And technologies can also allow patients to follow the audit trail of their own records.

We, patients, should be the ones to decide how much risk to our privacy we wish to take for our medical care, as amassing so much centralized data, inevitably puts the data at risk for breaches of all sorts. As a society, we need to guard against setting up mechanisms that could potentially be abused in ways that J. Edgar Hoover did with government data or as warned against by George Orwell. There are many ways in which medical data can be used against us, such as for employment, insurance coverage, etc. Note (in office) NPR's enclosed reporting of a case before the Supreme Court where the Federal government violated its own HIPAA laws and did not want to pay economic damages to the pilot whose medical privacy was violated and his HIV status disclosed. Once data is "outed," the damage is done.

Since there is no technology that can guarantee keeping data from hackers, nor laws that can totally protect data from misuse or breach, patients must be able to choose which data, if any at all, should go into an electronic exchange. (Data left out could be indicated with an asterisk.) If the HIE (Health Information Exchange) systems have to answer directly to

patients to process their data, they will be more careful about maintaining their security and privacy systems over time, particularly, as their definition of a breach undercuts their security provisions: "To compromise the security or privacy of PHI means to pose a significant risk of financial, reputational, or other harm to the individual whose PHI (protected health information) is involved." Who will decide if embarrassment rises to the level of *significance*? Will a patient have to go to court to argue that the breach was *significant* enough to even be notified? This provision protects the businesses, governments and even providers of the HIE, but how does it protect the patient? Also their audit policy is after the fact.

There are two arms of the consent model for the HIE that need to be addressed. One is the consent for use by providers, and the other is that for payment, operations, research and federal and state agencies. Please note that the HIPAA form, that patients are asked to sign, really just notifies patients that their data can be accessed by many business employees as long as they conform to the HIPAA privacy regulations. Most patients know that their doctor cannot talk to their mother without their consent, but they do not know that the doctor's accountant, for example, can see their record without their consent, as long as that person is a "business entity" conforming to HIPAA, which is, in fact, how the HITE-CT will be formatted.

It is hoped that the consent policy of the HIE will be changed to one of OPT- IN with *restrictions*, meaning that no data at *all* goes into the exchange for *any* purpose: TPO (treatment, payment operations), public health, research, quality control without the consent of the patient. (Restrictions would mean that the patient can choose which of their data goes into the exchange.) The all or nothing current consent policy of the HIE would make it easier for providers and the systems but would put patients over a barrel to force them into the exchange to receive treatment. Patients need to give consent for a *specific* provider to see their records, not to thousands across the country who cannot be stopped from accessing and downloading a record at least once. Medical records were often destroyed after seven years; now they will be permanent, and an error may not be removed but just addendum added. Secondly, it is hoped that the legislation of CT will be changed to require only *unidentifiable* (not easy to achieve) data be sent to the Dept. of Public Health, except in very limited medical circumstances such as the reporting of tuberculosis and other very contagious diseases.

The current OPT-OUT policy means that patients can opt-out of their data being "disclosed" to other *providers*. However, patients may not be able to not opt-out of their data being seen by many other business *employees* for treatment, payment, operations (see the long list of what is included), quality control, public health, research, etc. It is not clear if patients can opt-out of their data being seen in an emergency, nor what will be the exact status of "Sensitive" information (mental health, HIV status, substance abuse, etc.) in terms of it being seen by Public Health and possibly during TPO access. By law, the "Sensitive" data should be removed from a record for TPO use, unless the patient gives consent to release it. However, it is difficult to remove all mention of sensitive data from a record, and actually, a provider needs that data to treat a patient.

As it stands now, a provider does not even have to grant a patient's request to keep their data out of the exchange totally or to keep some data private unless it is that specifically mandated by law, regarding "sensitive" data. (Will abortion data be kept out of a women's OB-GYN record, as it is listed first in her record, by a numbering system that is standard to the record?) And how would you feel about all that personal information in your child or teenager's pediatrician's record going into

the exchange. Should that end up neatly typed in a record following a child for life. Does the US government need to know about a child's bedwetting if they apply to be a Navy SEAL?

Apparently, we have these threats to our privacy because in 1996, the HIPAA statute expanded law enforcement and public health access to patients' data without their consent. Then in 2002-3, Health and Human Services ruled that patient data can be serviced and accessed by many business entities for providers and insurance companies without explicit patient consent, as long as they sign privacy agreements and are compliant with the HIPAA privacy regulations. The HITECH Act of The American Reinvestment and Recovery Act of 2009 (ARRA, The Stimulus Bill) and the Patient Protection and Affordable Care Act (PPACA)and CT legislation have further expanded what must be sent to Public Health and the federal government without patient consent. They currently mandate that "meaningful use" data (problem list, meds, labs, allergies) of Medicaid and Medicare patients go the federal government which hopes to receive all patients' data, as part of the Nationwide Health information Network (NHIN) of which the HIE is a precursor. These uses of patient data may be legal, but are they constitutional? The government cannot search your house without a warrant, but can have access to one's most intimate private information without one's consent. I guess the laws are functioning as a global warrant on everybody. As one example online, Stamford Hospital says that patient records will be released if the "U.S. Department of Health and Human Services (or its contractors) asks for it for legal reasons or to review some special problem."

As for the Connecticut laws, HB 6652, PA 11-61, Sec. 143, (b) mandates that hospitals send our "identifiable inpatient discharge data and emergency department data to the Office of Health Care Access" ... of the DPH and "may be submitted through a contractual arrangement with an intermediary;" (c) that at least some of our outpatient data be sent by 2015 as well, without our consent; (d) "The office may release de-identified data" which is not reassuring, as even the federal government acknowledges data can be re-identified fairly easily; (e) the state Comptroller can access the data with permission. So this law seems to mandate that if I have an abortion, a private company may process my data and the CT Dept. of Public Health will have access to my most personal information. If it is determined that abortion is classified as "Sensitive" Protected Health Information (PHI), I do not know if it will go to the state in an identifiable form, but other diagnoses will surely go to the state. What about mental health admissions, will they go to the state as well?

HB 6678 PA 09-232 Sec. 7 calls for a tumor registry for all cancers. The state also wants occupational, demographic, etc. data. It is not clear whether this is identifiable data or not. However, (d) says that the DPH "may enter into a contract for the storage, holding and maintenance of the tissue samples under its control and management." So now the state of CT owns our body parts? What if the state rules or someone surreptitiously decides to do DNA testing on our tissue? Would patients even know, as the tissue is out of their control?

The DPH website cites HB 6678 PA 09232 Sec. 74-77 as one of the laws underpinning their work. Sec. 77 (a) (1) (A) calls for an "electronic health record that provides access in real–time to a patient's complete health record," (D) "electronic alerts and reminders to health care providers to improve compliance with best practices, promote regular screening and other preventive practices, and facilitate diagnoses and treatments" and (F) tools to allow for the collection, analysis and reporting of data on adverse events, near misses and the quality and efficiency of care, patient satisfaction and other healthcare-related performance measures." So does this mean that our State

is going to oversee and monitor our treatment and in a sense, be in the exam room with us and our providers? Will governments be using the data to decide which treatments will be *available* and to which *age* groups? Would it be possible to do this without knowing our identities?

Also it seems that the HIE also intends to use the whole record, not just that used for "meaningful use." The website also cites PA 10-117, Substitute Senate Bill 428, sec. 82 (e) that says that the health information technology plan is for the "implementation of an integrated state-wide electronic health information infrastructure for the sharing of electronic health information among health care facilities, health care professionals, public and private payers, state and federal agencies and patients." So which state and federal agencies will have access to our medical records without our explicit consent, as the HIE will comply with "existing laws, i.e. Public Health"?

The DPH website under Policies and Procedures, Meaningful Use and Public Health explains that it will use the HIE according to the provisions in ARRA and the HITECH Act. It states that "meaningful use is defined in a specific way, requiring fifteen "core" and ten "menu" criteria. Of the ten menu options, three require reporting to public health:"

"Submit electronic data to public health immunization registries/systems."

"Provide electronic submission of reportable lab results to public health agencies" - This is a very long list, including lead levels, which goes way beyond communicable diseases. And it may mean that your teenager's sexually transmitted infection lab results will be reported directly to the CT DPH, probably in an identifiable form. Does any *newborn* lab or DNA data go automatically to the Dept. of Public health for its surveillance or other programs?

"Provide electronic syndromic surveillance data to public health agencies." - This could mean that identifiable patient data on weight, smoking, etc. will be seen by the DPH. How broad will the definition be, of what medical data falls under surveillance, without our consent?

Also there is the whole issue of patient privacy regarding their prescription drug information going to pharmaceutical companies, government, etc. and their use of controlled substances going to the State of Connecticut and possibly many providers too. And there is the issue of who will be held liable for the inevitable errors in the electronic record; the emergency room physician treating the comatose patient with a record from the exchange or the primary care provider.

Thank you very much for reading this!

[redacted]

From: Susan Israel [redacted]
Sent: Saturday, March 24, 2012 9:15 AM
To: PHC Testimony
Subject: SB 368

[redacted]

The Committee on Public Health

Testimony on Raised Bill 368

March 16, 2012

I am Susan Israel, a physician, I would like to commend and thank the members of the Public Health Committee for putting forth 368 to give patient's control over access to their medical information through the Exchange.

The enactment of 368 would put CT in the forefront of patient rights, and would be on the right side of history. It would be more cost effective to do this now, while the exchange is being formed, rather than redoing it later, after patients become aware of all those who can see their records without their explicit consent and demand changes to the exchange. Also the best way for the privacy and security provisions to be maintained over time, would be for the Exchange to answer directly to patients, who would have the choice to participate or not, in a free market way. Without 368, the Exchange will be operating, far more, on a captive audience model.

I would hope that the policy makers would fully educate the patient as to their definition of a breach, which to quote directly is: to "compromise the security or privacy of PHI (protected health information) means to pose a significant risk of financial, reputational or other harm to the individual ..." However, individuals would not even be notified unless

someone else thinks it is harmful enough to tell them. Apparently, this definition is needed to facilitate the processing of the records by the providers and businesses involved because of worry over liability issues. I would also like to point out that the audit trail is done after the fact periodically and there is nothing to stop thousands of providers from accessing any patient's data at least once. No one would hire a babysitter without out meeting the person. But we are being told that our most intimate information will be processed by people we do not know, according to the policies of appointees and according to laws most are not aware of. The philosophy underlying these actions is that the Exchange is needed to carry out health care policies that are in our best interest, whether or not we know it, or agree.

The pentagon cannot protect its computers, but we are being told not to worry. All details of the safeguards and technologies, used in the Exchange, need to be disclosed and made transparent to the public *before* their records are made part of it. Patients should be the ones to decide how much risk to their privacy they wish to take in order to receive treatment.

There are, however, technologies being put into place nationally and being developed that can allow patients control over what part of their medical data is seen and by whom. The organizations, Patient Privacy Rights and the bipartisan Coalition for Patient Privacy, are working on these issues. They are having a Summit in Washington, DC in June to bring this knowledge to the American public.

Thank you very much for this opportunity.